CyberLaw

A Presentation to the
Naval Postgraduate School
Monterey, California
January 7, 2005

Daniel J. Ryan
ryand@ndu.edu

National Defense University

Legal Stuff – Read Carefully

- This presentation is designed to provide authoritative information with regard to the subject matter covered. The information is provided for your information only and should not be relied upon as legal advice. This presentation makes no warranties, express or implied, based on the information it contains. Nothing in this presentation constitutes the establishment of an attorney-client relationship between you and Daniel J. Ryan, Esquire. Please remember that laws may differ substantially in individual situations or in different states, so you should never rely on legal or other materials from this or any other slide presentation without first seeking advice about your particular situation from an attorney licensed to practice in the appropriate jurisdiction. Nothing contained in this presentation should be construed to constitute a recommendation or endorsement of any company or firm, product, or service.

We face new choices

Select One

Security

Privacy

Networks and CyberCrime

- Your employees hack your computers
- They write malicious code and destroy valuable information assets
- Employees download MP3's and movies, gobbling up bandwidth and violating copyrights
- Employees download pornography and share it with other students via your e-mail system
- Employee downloads child pornography and stores it on the university's network
- Employee moonlights by running a personal business form her office workstation
- Employee steals your intellectual capital and sells it on eBay
- Employee uses your computers to embezzle from you
- Disgruntled Employee sabotages your network

Problems => lawsuits

- Privacy – especially personal information
- Property – copyright and patent infringement
- Torts – defamation, downstream liability
- Contracts – digital signatures
- Administrative and Regulatory Law
- Criminal Law and Procedure
- Other Fascinating Issues

It’s a “target rich” environment!

Federal CyberLaw

- 18 USC 1029 Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030 Computer Fraud and Abuse Act
- 18 USC 1362 Communication Lines, Stations or Systems
- 18 USC 2511 Electronic Communications Privacy Act
- 18 USC 2701 Unlawful Access to Stored Communications
- 18 USC 2702 Disclosure of Contents
- 18 USC 2703 Requirements for Government Access
- 18 USC 793 Espionage
- 15 USC 1644 Consumer Credit Protection
- 17 USC 101 et seq. Copyright
- 18 USC 1831-2 Economic Espionage

Monitoring Network Operations

- **Two situations:**
  - **Everyday routine operations**

  - vs -

  - **Incident response**

Auditing and Monitoring Network Activity

- **Network monitoring**
  - **Real-time acquisition and contemporaneous or subsequent analysis of network communications**
    - **Ethereal, tcpdump, NIDS such as Snort, email server virus scanners, etc.**

- vs -

- **Stored electronic files**
  - **Sysop's and Network Administrator's review of stored network communications and network or host logs**

Criminal Activity on Networks

- **Illegal Surveillance**
  - **Wiretap Act (18 U.S.C. § 2511)**
  - **Pen/Trap Statute (18 U.S.C. § 3121)**
  - **Electronic Communications Privacy Act (18 U.S.C. § 2701)**
- **Network Crimes**
  - **Computer Fraud and Abuse Act (18 U.S.C. § 1030)**
- **Using a Network to Commit Traditional Crimes**
  - **Criminal copyright/trade secret violations**
  - **Threats, stalking and harassment**
  - **Child pornography**
  - **Fraud, embezzlement, money laundering, counterfeiting, extortion**

Illegal Surveillance

- Wiretap Act (Title III - ECPA I)
  - real-time interception of electronic, voice and wire communication content contemporaneous with transmission
    - Examples: packet data payloads, email subject lines

- Pen Register/Trap and Trace Statute (Pen/Trap)
  - installation or use of a device that decodes or intercepts electronic and wire communication non-content such as routing or addressing information
    - Examples: packet headers, email bang lines

- The Stored Communications Act (ECPA II)
  - Covers illegal access to certain stored voice and electronic communication service facilities

Wiretap Act

- Prohibits intercepting the content of communications during delivery unless an exception applies

- Four important exceptions:
  - Consent [18 U.S.C. § 2511(2)(c)]
  - Provider exception [18 U.S.C. § 2511(2)(a)(i)]
  - Computer Trespasser [18 U.S.C. § 2511(2)(i)]
  - Publicly Accessible [18 U.S.C. § 2511(2)(g)(i)]

Consent Exception

- **Two types of consent:**
  - **Party consent**
  - **Implied or express consent by a non-party**

Party Consent

- Lawful to intercept if you are a party to the communication
  - Who is a “party” to computer network communications?
    - Some cases suggest that the owner of a computer network (and the owner’s agents) are a “party” to communications sent to and from the network.

But: What about the pass-through victim?

Implied and Express Consent

- **Obtain express or implied consent to monitor prior to interception**
  - **Implied: Banner on the login screen**
  - **Express: Obtain written consent of authorized users**

But: Trespassers unlikely to see banners and won’t give express consent

Provider Exception

- **Allows network owners (and their agents) to conduct reasonable interception, use & disclose:**
  - **To protect provider's "rights or property"**
  - **When done in normal course of business while engaged in any activity which is a necessary incident to the rendition of service**

But: Does not permit unlimited monitoring

But: You cannot use provider exception to prospectively gather evidence for law enforcement

Computer Trespasser Exception

- USA PATRIOT Act modification to Wiretap Act
- Allows law enforcement to intercept communications to or from “computer trespassers”
  - A “computer trespasser” is a person who accesses a computer without authorization
    - excludes persons known by the provider to have an existing contractual relationship with the provider for use of the system
    - someone exceeding their authorized use is not a trespasser
  - Applies only if the provider authorizes the interception
  - Interception performed by law enforcement or its agent

But: Expires Dec. 31, 2005 (unless Patriot Act extended)

Publicly Accessible Exception

- **Permits interception of communications that are readily accessible to the general public**
  - **Example: public message board postings**

But: Does not apply to private forums

- **private chat session within public chat room**
- **if bannered, consent may apply**

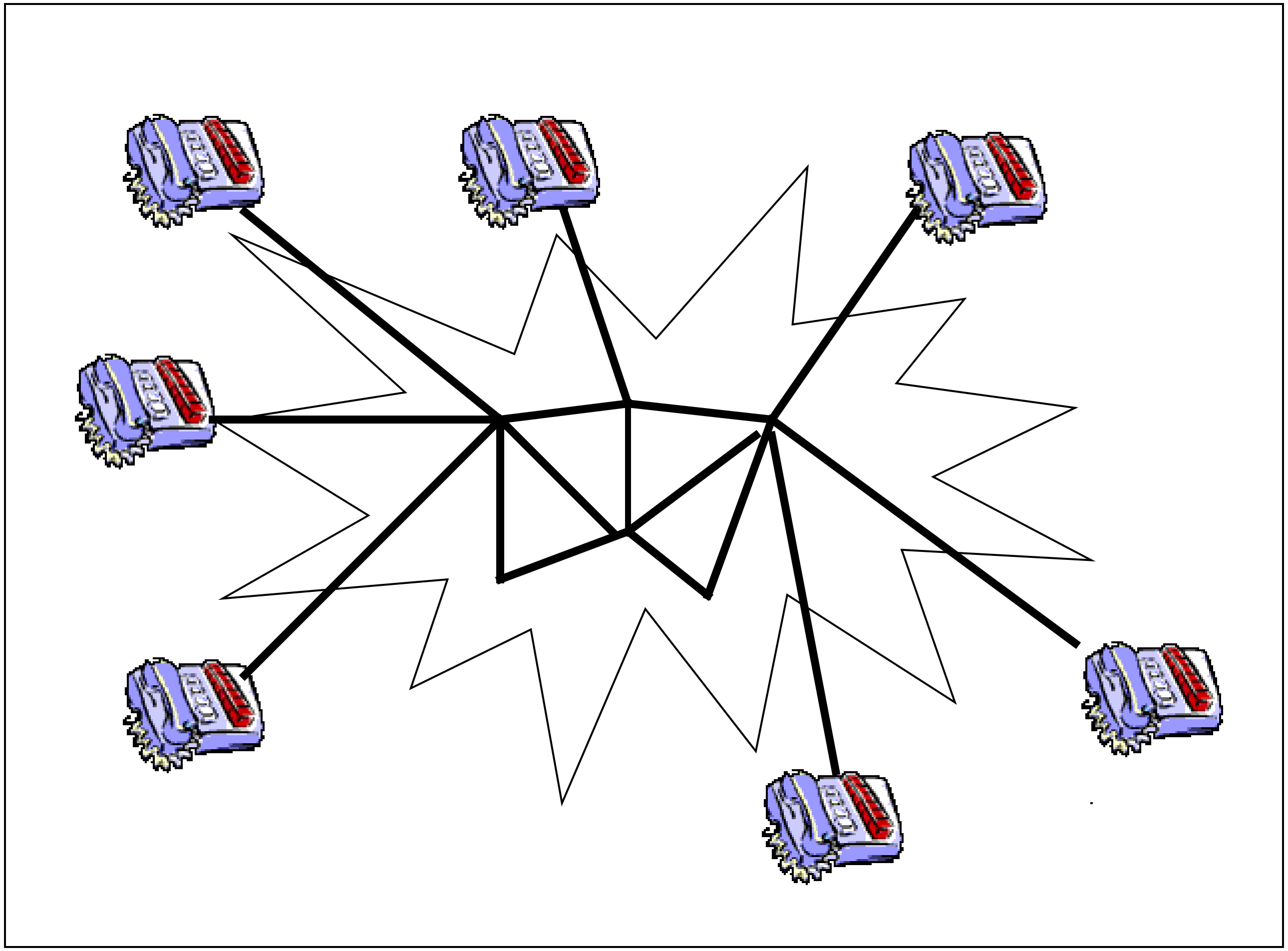
PEN/TRAP Statute

- **Prohibits intercepting the non-content parts of communications streaming across a network unless an exception applies**
- **Broad authority for providers to use pen/trap devices:**
  - **For operations, maintenance, or testing;**
  - **To protect rights or property;**
  - **To protect users from abuse or unlawful use;**
  - **To record communication initiation and completion to protect rights or property, another provider furnishing service and users from fraudulent, unlawful or abusive use of service; and**
  - **Where the implied or express consent of the user has been obtained.**

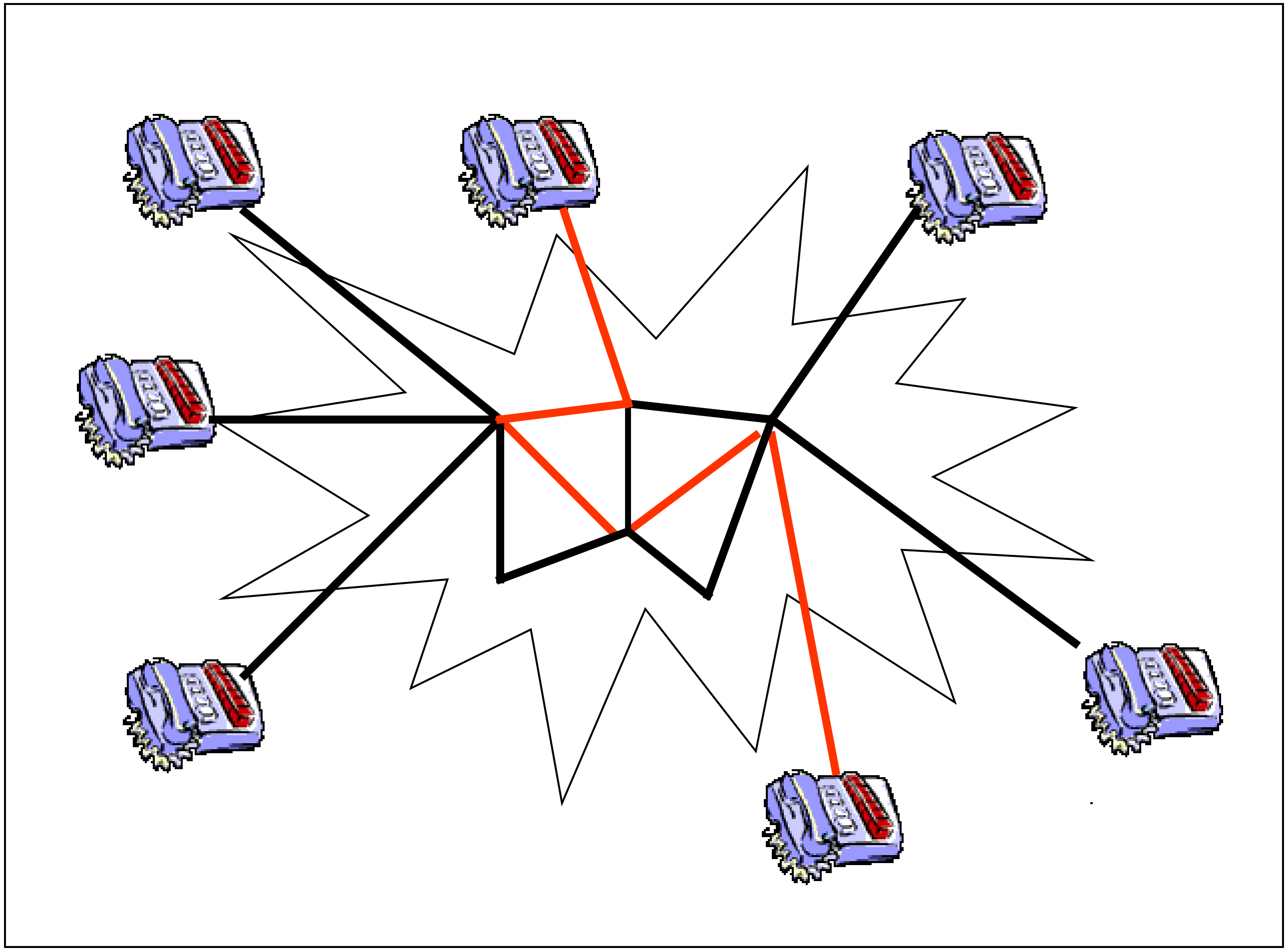
Stored Communications

- **18 USC § 2701 prohibits accessing electronic or wire communications in “electronic storage” without or in excess of authorization**
  - **Example: obtaining, altering or deleting unretrieved email**
- **Provider exception:**
  - **§ 2701 does not apply to conduct authorized by the person or entity providing an electronic or wire service**
  - **Example: e-mail virus scanning**

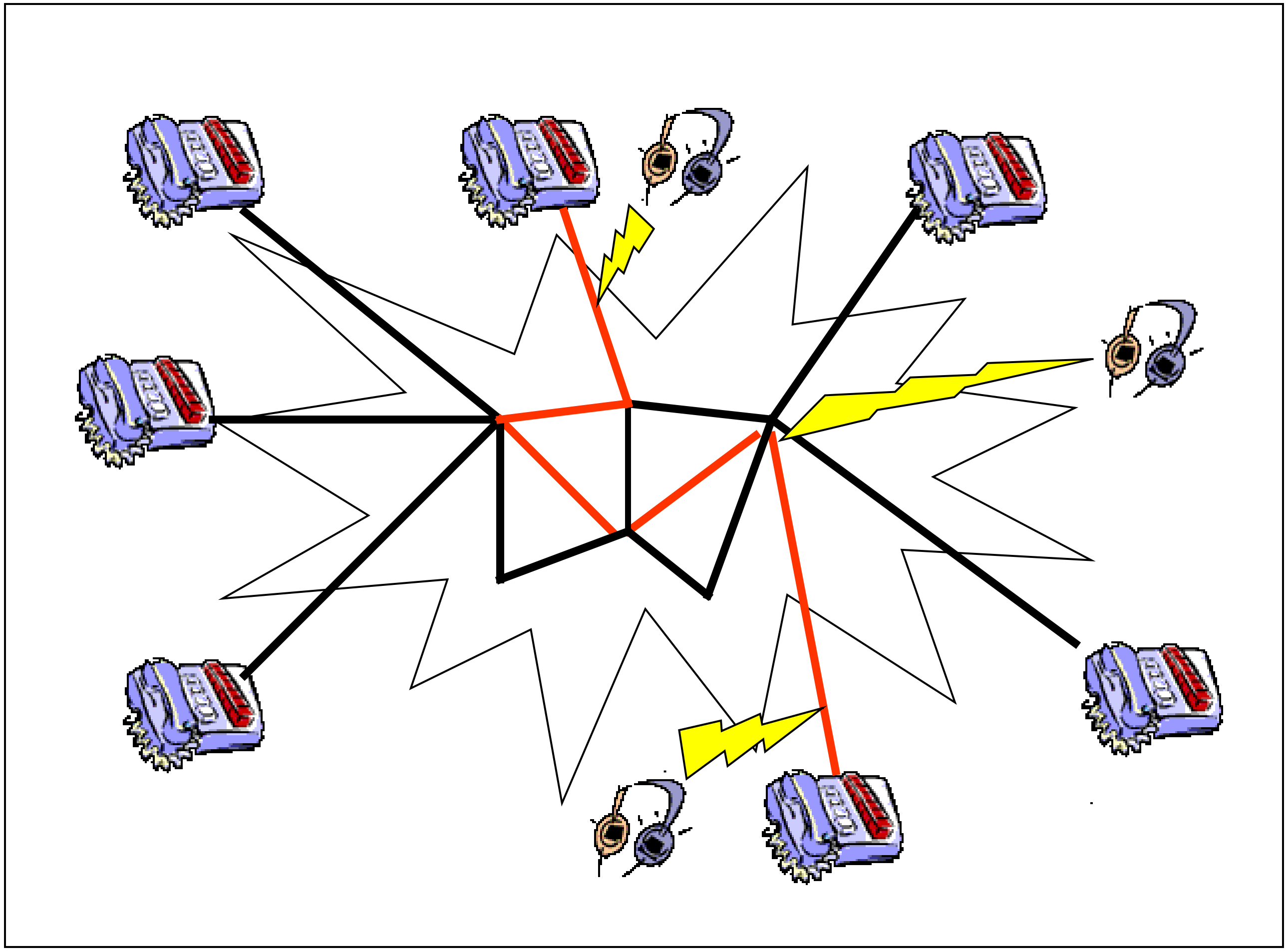
Circuit Switching



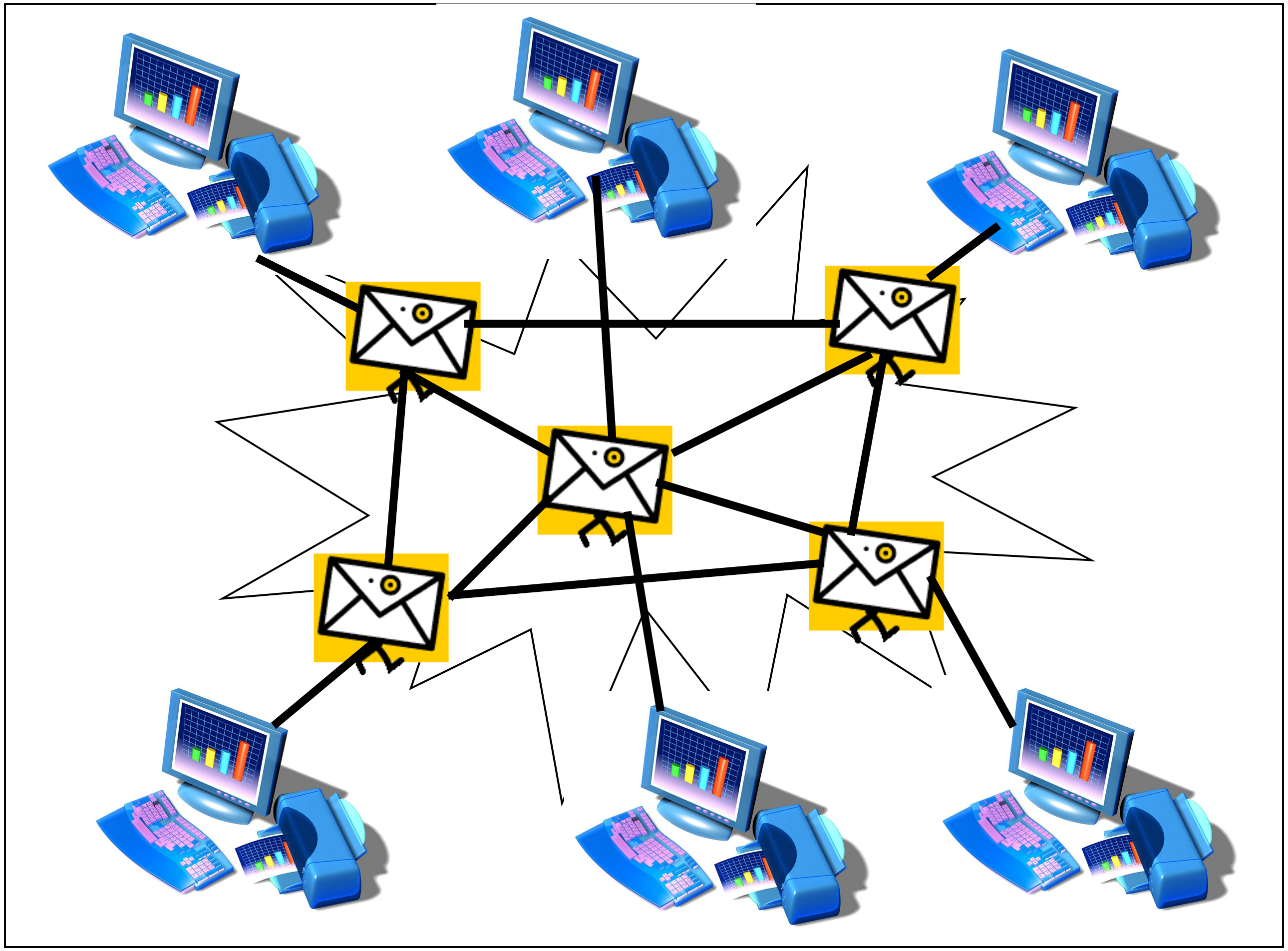
Circuit Switching



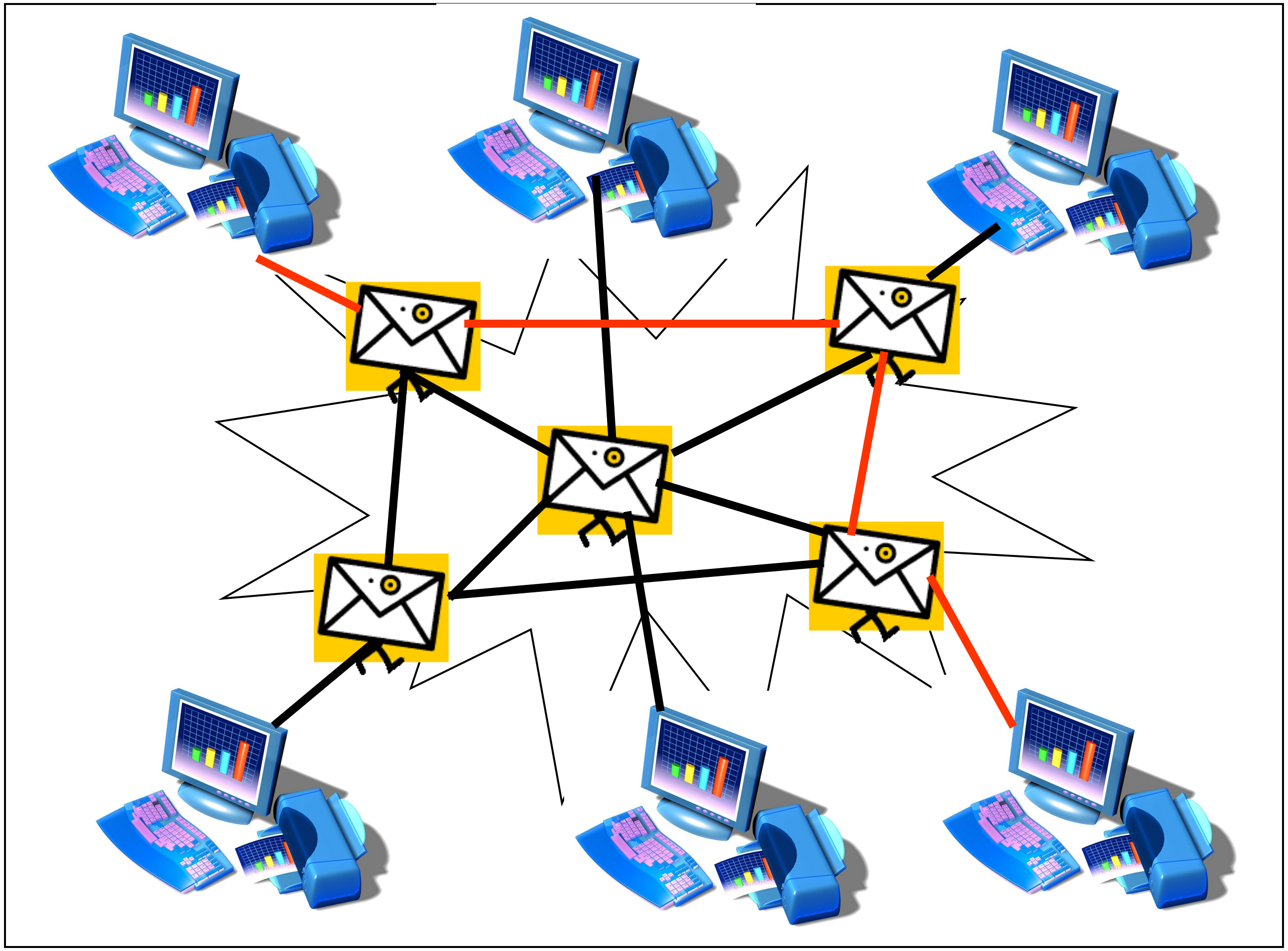
Circuit Switching



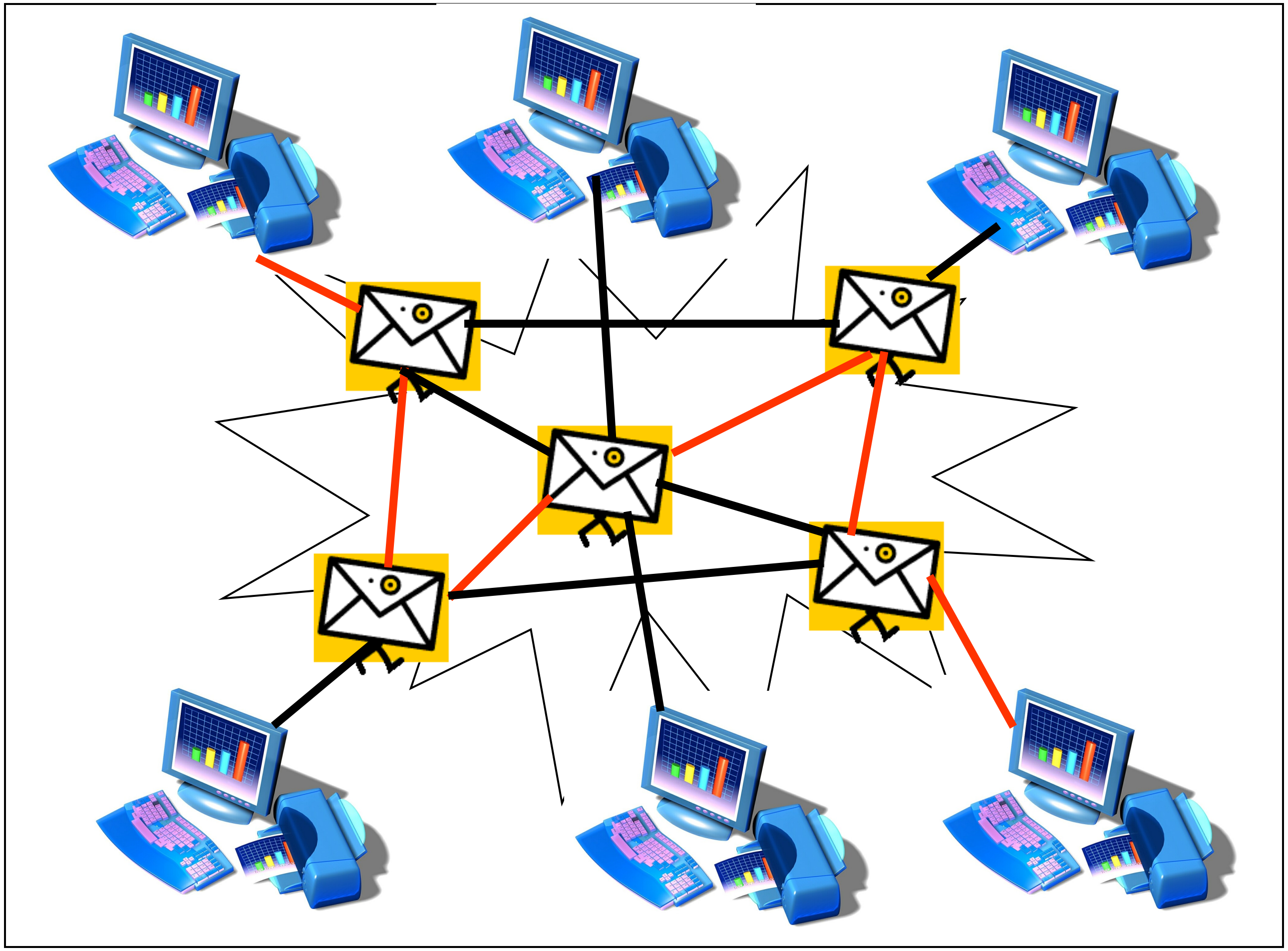
Packet Switching



Packet Switching



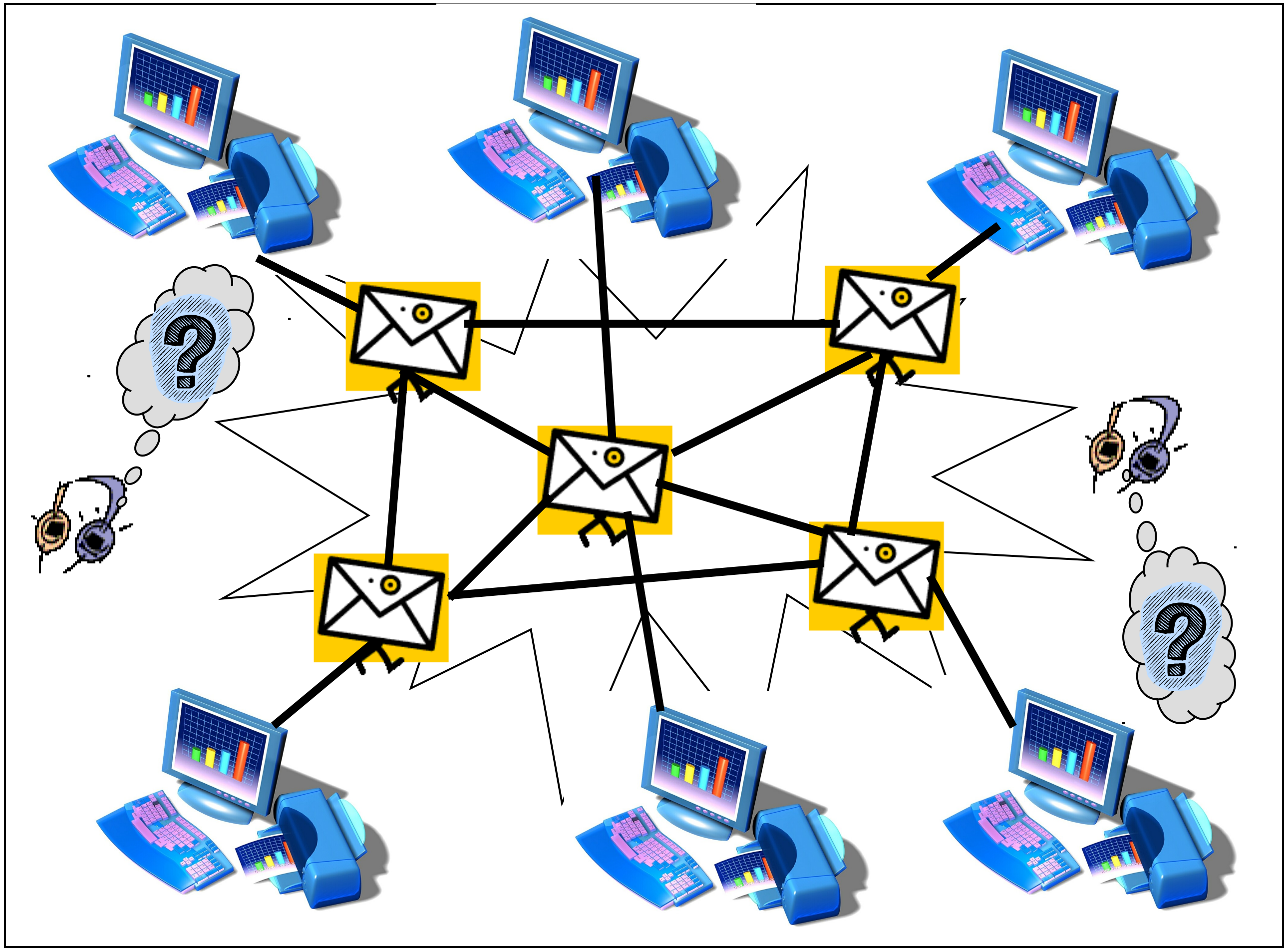
Packet Switching



Daniel J. Ryan
ryand@ndu.edu

National Defense University

Packet Switching



Key Cases

- Steve Jackson Games v. USSS
- Konop v. Hawaiian Airlines
- US v. Scarfo
- US v. Steiger
- Thompson v. Thompson
- US v. Councilman
- Theofel v. Farley-Jones

Incident Response

- Criminal activity on the network
  - Network Crime
  - Other types of crime
- Call in law enforcement
- Keep records that will quantify the damages caused by the incident
- Log traffic data
- Consider imaging affected systems

Remember: Digital forensics is not for amateurs

Preparing in Advance

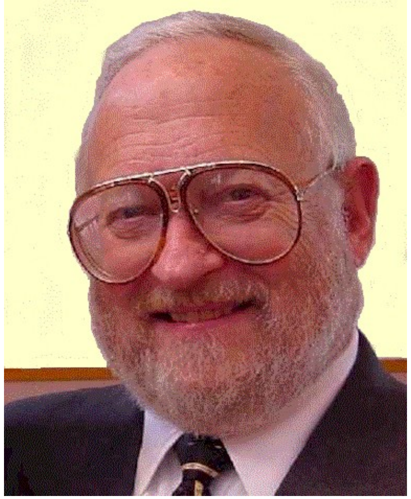
- Instill healthy concern and caution
  - Management
    - Instill concern and illustrate threat
    - Emphasize planning, policies and procedure
  - CERT Team
    - Trained and equipped
  - Sys admins and network engineers
    - Instill caution
  - All employees
    - What to look for
    - Who to call

Civil CyberLaw

- Privacy
  - E-mail privacy
  - Adult materials
  - Spam
- Torts
  - Defamation
  - Tortious interference with business
  - Downstream liability
- Intellectual Property
  - Copyrights, patents, trade secrets, trade dress

- Contract Law
  - Electronic signatures
  - e-commerce and e-government
- Jurisdiction in cyberspace
- Administrative Law and Regulation
- Business and tax law
- Professional liability
  - Erroneous information
  - Professionals
  - Professors

Thank You!



Daniel J. Ryan
Professor
Information Resources
Management College
National Defense University

202.685.2843 v

ryand@ndu.edu
www.danjryan.com